UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/501,902	02/10/2000	Philip L. Bohannon	11-20-1-2-2	4531

22046 7590 06/14/2004

LUCENT TECHNOLOGIES INC.
DOCKET ADMINISTRATOR
101 CRAWFORDS CORNER ROAD - ROOM 3J-219
HOLMDEL, NJ 07733

EXAMINER	
ZIA, SYED	

ART UNIT	PAPER NUMBER
2131	6

DATE MAILED: 06/14/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/501,902	BOHANNON ET AL.	
	Examiner	Art Unit	
	Syed Zia	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *29 March 2004*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-10 and 24-39* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-10, and 24-39* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Response to Amendment

This office action is in response to arguments filed on March 29, 2004 (Paper No. 5). Original application contained Claims 1-39. Applicant amended Claims 1, 5, 7, 24, 29-31, 34, and 37. Applicant cancelled Claims 11-23. The amendment filed have been entered and made of record. Presently pending claims are 1-10, and 24-39.

Claim Rejections - 35 USC § 112

Regarding **Claim Rejection Based Upon *35 USC § 112*** examiner still asserts that specification does not explicitly describe nor is sufficiently clear for one of ordinary skill in art to recognize the steps as recited in claims 4, and 5 (Please refer previous office action [Paper No. 4] for detail description).

Response to Arguments

Applicant's arguments filed on March 29, 2004 (Paper No. 5) have been fully considered but they are not persuasive because of the following reasons:

Regarding independent and dependent Claims applicants argued that the cited prior arts (CPA) [Gibbs et al. U.S. Patent No. 6,085,321] do not teach, " *a function to the varying*

parameters in order to generate a set of indices which in dices, in turn, are used to access the stored cryptographic shares upon which the cryptographic key is generated ".

This is not found persuasive. CPA clearly teach system and method comprising a mechanism for removably coupling a portable memory to the system, to provide a coupled portable memory, in which the coupling provides data communication between the memory and the system. An associated information reader provides read information, which is unique to the coupled portable memory. An information selector is provided together with a mechanism for combining the read information with the selected information, creating combined information, which is a single data string. There is a mechanism for generating a cryptographic key set, which utilizes the combined information. The key set comprises at least one encryption key and one decryption key. The cryptographic key is stored in the coupled portable memory, and the encryption key can be stored in a data storage section of the system. There is also a mechanism for encrypting the selected information, utilizing the encryption key, together with a mechanism for reading the decryption key from the coupled portable memory. An arrangement is provided for decrypting the encrypted information.

As a result, CPA does implement and teaches a system and method for managing, generation and use of cryptographic keys for computer security applications.

Applicants clearly have failed to explicitly identify specific claim limitations, which would define a patentable distinction over prior arts.

The examiner is not trying to teach the invention but is merely trying to interpret the claim language in its broadest and reasonable meaning. The examiner will not interpret to read narrowly the claim language to read exactly from the specification, but will interpret the claim

language in the broadest reasonable interpretation in view of the specification. Therefore, the examiner asserts that APA does teach or suggest the subject matter broadly recited in independent Claims 1, 24, 34, 37 and in subsequent dependent Claims 2-10, 25-33, 35-36, and 38-39. Accordingly, rejections for claims 1-10, and 24-39 are respectfully maintained.

Claim Rejections - 35 USC § 102

1. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in a patent granted on an application for patent by another filed in the United States before the invention thereof by the applicant for patent, or on an international application by another who has fulfilled the requirements of paragraphs (1), (2), and (4) of section 371(c) of this title before the invention thereof by the applicant for patent.

The changes made to 35 U.S.C. 102(e) by the American Inventors Protection Act of 1999 (AIPA) and the Intellectual Property and High Technology Technical Amendments Act of 2002 do not apply when the reference is a U.S. patent resulting directly or indirectly from an international application filed before November 29, 2000. Therefore, the prior art date of the

reference is determined under 35 U.S.C. 102(e) prior to the amendment by the AIPA (pre-AIPA 35 U.S.C. 102(e)).

2. Claims 1-10, 34, 37 and 39 rejected under 35 U.S.C. 102(e) as being anticipated by Kara (U.S. Patent No. 5,802,175).

3. With respect to claim 1, Kara teach a method for generating a cryptographic key (see abstract; col. 2, lines 42-57) using at least one parameter comprising the steps of:

generating at least one index as a function of said at least one parameter, said one parameter being from a plurality of varying parameters (col.4 line 62 to line 67);

retrieving at least one cryptographic share from a memory location identified as a function of said at least one parameter (see col. 2, lines 42-67); and

generating a cryptographic key based on said at least one cryptographic share (see col. 2, lines 42-67).

4. Claim 2 rejected as above in rejecting claim 1, wherein said at least one retrieved cryptographic share is encrypted, said method further comprising the step of:

decrypting said at least one cryptographic share (see col. 3, lines 1-25).

5. Claim 3 rejected as above in rejecting claim 2, wherein said step of decrypting comprises the step of:

decrypting using a value computed as a function of said at least one parameter (see col. 3, lines 44-57).

6. Claim 4 rejected as above in rejecting claim 1, wherein at least one retrieved cryptographic share is compressed, said method further comprising the step of:

decompressing said least one cryptographic share (see col. 5, lines 13-26).

7. Claim 5 rejected as above in rejecting claim 4, wherein said step of decompressing comprises the step of:

decompressing said at least one cryptographic share using said index to said memory location (see col. 5, lines 13-26; col. 6,lines 42-57).

8. Claim 6 rejected as above in rejecting claim 1, wherein said at least one parameter represents at least one measurement of a physical property (see col. 4, lines 62-67 to col. 5, lines 1-6).

9. Claim 7 rejected as above in rejecting claim 1, wherein the plurality of varying parameters change from one said generation of said cryptographic key to a next generation of said cryptographic key (col.2 line 42 to line 67, col. 3 line 1 to line 25, and col. 6 line 30 to line 64);

10. Claim 8 rejected as above in rejecting claim 7, further comprising the step of:

retrieving a cryptographic share from a memory location in the vicinity of said memory location identified by said index (see col. 6, lines 42-64).

11. Claim 9 rejected as above in rejecting claim 7, wherein said step of generating at least one index comprises the step of generating the same index for a set of parameter values (see col. 6, lines 42-64).

12. Claim 10 rejected as above in rejecting claim 9, wherein said set of parameter values are within a predetermined range of values (see col. 6, lines 17-41).

13. With respect to claim 34, a method for generating a cryptographic key using a plurality of varying parameters said varying parameters representing physical measurements, said method comprising the steps of: for each of said plurality of parameters; generating at least one index using said parameter; retrieving an encrypted cryptographic share from a memory location as a function of said at least one index; decrypting said encrypted cryptographic share with a function of said parameter; and generating a cryptographic key using said decrypted cryptographic shares (see abstract; col. 2, lines 42-67 to col. 3, lines 1-25; col. 4 line 62 to line 67, and col. 6, lines 30-64).

14. With respect to claim 37, a data structure for use in generating a cryptographic key based on n parameters representing physical measurements, said data structure comprising: n storage locations each associated with a respective one of said n parameters, each particular storage location containing an encrypted cryptographic share which was encrypted using an expected values of a function of the parameter associated with said particular storage location, each said n storage location being associated with at least one index of a plurality of indices, where said plurality of indices are generated using said physical measurements (see col. 2, lines 23-67 to col. 3,lines 1-57).

15. Claim 39 rejected as above in rejecting claim 37, wherein said cryptographic key may be generated using less than *n* cryptographic shares (se col. 3, lines 1-25).

Claim Rejections - 35 USC § 103

16. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

17. Claims 24, 26-27, 29-33 and 35 rejected under 35 U.S.C. 103(a) as being unpatentable over Kara U.S. Patent No. 5,802,175 in view of Brown et al. U.S. Patent No. 5,557,686 ('Brown' hereinafter).

18. With respect to claim 24, Kara teach a method for generating a cryptographic key (see abstract; col. 2, lines 42-57) comprising the steps of:

generating a cryptographic key using said cryptographic shares (see col. 2, lines 42-57).

Kara does not explicitly disclose measuring a plurality of keystroke features during entry of a password and retrieving from a data structure a plurality of cryptographic shares as a function of said plurality of keystroke features.

Brown disclose measuring a plurality of keystroke features during entry of a password by

generating a plurality of indices using said plurality of keystroke features (see col. 2, lines 12-56; col. 3, lines 35-41); and

retrieving from a data structure a plurality of cryptographic shares as a function of said plurality of indices (see col. 2, lines 12-56; col. 3, lines 35-41, and col. 4 line 63 to line 67).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of Brown within the system of Kara to arrive at the invention as claimed because the implementation of measuring the keystroke features during entry of a

password of a user would improve the ability of detecting the users who are trying to access the system, and further increase the level of security of the combined system.

19. As to claim 26, Kara does not explicitly show said cryptographic shares represent vectors. However, Brown teach wherein said cryptographic shares represent vectors (see col. 2, lines 12-51; col. 5, lines 25-29; col. 6, lines 61-67). It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine Kara in view of Brown for the same reasons set forth in claim 24 above.

rejected as above in rejecting claim 24, wherein said cryptographic shares represent vectors.

20. Claim 27 rejected as above in rejecting claim 24, wherein said cryptographic shares are compressed.

21. Claim 29 rejected as above in rejecting claim 24, wherein said plurality of keystroke features vary from said generating of said cryptographic key to a next generation of said cryptographic key (see col. 2, lines 12-56; col. 3, lines 1-41, and col. 6 line 30 to line 64).

22. Claim 30 rejected as above in rejecting claim 29 24, wherein said step of generating a plurality of indices as a function of said keystroke features comprises the step of:

for each of said keystroke features, generating one of two indices as a function of a threshold value, h_i , where said function is defined by:

$f(\varphi_1, \varphi_2, \ldots \varphi_m) = \{\psi_1, \psi_2, \ldots \psi_m\} \epsilon \{0,1\}^m$ where φ represents said keystroke features, ψ represents said indices, m is a particular number of measured features associated with said password; and ψ_i $\{0$ if $\varphi_i < h_i$
1 if $\varphi i < h_i$
(col. 2, lines 12-56; col.3 lines 35-41).

23. Claim 31 rejected as above in rejecting claim 29, wherein said step of generating a plurality of indices as a function of said keystroke features comprises the step of:

for each of said keystroke features, generating one of a plurality of indices as a function of a plurality of threshold values h_i, where said function is defined by:

$f(\varphi_1, \varphi_{2,} \ldots \varphi_m) = \{\psi_1, \psi_{2,} \ldots \psi_m\} \epsilon \{0,1\}^m$ where φ represents said keystroke features, ψ represents said indices, m is a particular number of measured features associated with said password; and ψ_i $\{0$ if $\varphi_i < h_i$
1 if $\varphi i < h_i$
(see col. 2, lines 12-56; col. 3 lines 35-41).

24. As per claim 32, Kara does not explicitly show decrypting said cryptographic shares using said password. However, Brown teach the use of a password (see col. 2, lines 52-56; col. 3, lines 35-41). It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine Kara in view of Brown for the same reasons set forth in claim 24 above.

25. Claim 33 rejected as above in rejecting claim 24, further comprising the steps of:

maintaining a history file containing information relating to prior successful key generation attempts and based on said history file, storing invalid cryptographic shares in data structure locations which are not expected to be accessed during subsequent legitimate key generation attempts (see col. 2, lines 42-67 to col. 3, lines 1-25).

26. Claim 35 rejected as above in rejecting claim 34, wherein said physical measurements are measurements of DNA.

27. Claims 25 and 28 are rejected under 35 U.S.C. 103(a) as being unpatentable over Kara U.S. Patent No. 5,802,175 in view of Brown et al. U.S. Patent No. 5,557,686 ('Brown' hereinafter) in further view of Herzber et al. U.S. Patent No. 5,625,692 ('Herzber' hereinafter).

28. As to claim 25, Kara and Brown teach the limitations as above as indicated in claim 24.

Kara and Brown do not explicitly disclose wherein said cryptographic shares represent points on a polynomial.

Herzber disclose cryptographic shares represent points on a polynomial (see col. 8, lines 10-21, 46-59; col. 16, lines 39-40)

It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of Kara and Brown with the system of Herzber to arrive at the invention as claimed because points on a polynomial which have been encrypted using the expected values indicated as the encryption key would further provide an increase level of security of the encryption key from being accessed or disclosed to unauthorized users attempting to gain access to the encryption key, further improving the security of the combined system by making it more difficult to decrypt the polynomial point with the decryption key.

29. As to claim 28, Kara and Brown teach the limitations as above as indicated in claim 27.

Kara and Brown do not explicitly disclose wherein said cryptographic shares comprise y values of points on a polynomial and the corresponding x values are derivable from a data structure location.

Herzber disclose cryptographic shares represent points on a polynomial (see col. 8, lines 10-21, 46-59; col. 16, lines 39-40)

It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of Kara and Brown with the system of Herzber to arrive at the invention as claimed because points on a polynomial which have been encrypted using the expected values indicated as the encryption key would further provide an increase level of security of the encryption key from being accessed or disclosed to unauthorized users attempting to gain access to the encryption key, further improving the security of the combined system by making it more difficult to decrypt the polynomial point with the decryption key.

30. Claims 36 and 38 are rejected under 35 U.S.C. 103(a) as being unpatentable over Kara U.S. Patent No. 5,802,175 in view of Herzberg et al. (U.S. Patent No. 5,625,692).

31. Kara teach claim 36 is rejected as above in rejecting claim 34.

Kara does not explicitly disclose said encrypted cryptographic share is a hash function.

Herzber disclose the use of a hash function (see col. 8, lines 26-30; col. 9,lines 35-42).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teaching of Herberg with the system of Kara to arrive at the invention as claimed because the implementation of a hash function would enable the cryptographic share to determine the position of a given value in the set of expected index values and to calculate the hash value for the given item, further extending the capabilities and increasing the level of security of the combined system.

32. Kara teach claim 38 is rejected as above in rejecting claim 37.

Kara does not explicitly disclose said encrypted cryptographic share is a hash function.

Herzber disclose the use of a hash function (see col. 8, lines 26-30; col. 9,lines 35-42).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teaching of Herberg with the system of Kara to arrive at the invention as claimed because the implementation of a hash function would enable the cryptographic share to determine the position of a given value in the set of expected index values and to calculate the hash value for the given item, further extending the capabilities and increasing the level of security of the combined system.

Conclusion

Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event,

however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Syed Zia whose telephone number is 703-305-3881. The examiner can normally be reached on Monday - Friday 9:00 AM to 5:00 PM EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 703-305-9648. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

sz
June 7, 2004

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100